

RECEIVED
CENTRAL FAX CENTER

APR 10 2006

DILLON & YUDELL LLP
ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO: Examiner Christian A. LaForgia		FROM: Matthew W. Baca, Reg. No. 42,277
ORGANIZATION: US Patent and Trademark Office		DATE: April 10, 2006
ART UNIT: 2131	CONFIRMATION NO.:	TOTAL NO. OF PAGES INCLUDING COVER: 21
FAX NUMBER: 571.273.8300		APPLICATION SERIAL NO: 09/696,518
ENCLOSED: Response to Notification of Non-Compliant Appeal Brief		ATTORNEY DOCKET NO: FR919990110US1

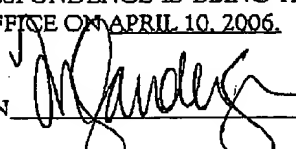
☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

CERTIFICATE OF FACSIMILE TRANSMISSION UNDER 37 C.F.R. § 1.8(A)

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING FACSIMILE TRANSMITTED TO THE U.S. PATENT AND TRADEMARK OFFICE ON APRIL 10, 2006.

SIGNATURE OF MICHELLE SANDERSON



This fax from the law firm of Dillon & Yudell LLP contains information that is confidential or privileged, or both. This information is intended only for the use of the individual or entity named on this fax cover letter. Any disclosure, copying, distribution or use of this information by any person other than the intended recipient is prohibited. If you have received this fax in error, please notify us by telephone immediately at 512.343.6116 so that we can arrange for the retrieval of the transmitted documents at no cost to you.

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

APR 10 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN RE APPLICATION OF: §
§
OLIVIER DAUDE § EXAMINER: CHRISTIAN A. LA FORGIA
§
SERIAL No.: 09/696,518 §
§
FILED: OCTOBER 25, 2000 § ART UNIT: 2131
§
FOR: M/S FOR PREVENTING §
UNAUTHORIZED SERVER §
INTERFERENCE IN AN §
INTERNET PROTOCOL §
NETWORK §

RESPONSE TO NOTIFICATION OF NON-COMPLIANT
APPEAL BRIEF UNDER 37 C.F.R. 41.37

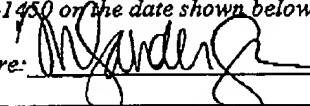
Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in response to a Notification of Non-Compliant Appeal Brief mailed on March 22, 2006 for the Appeal Brief filed on June 17, 2005. No fee is required to file this Compliant Appeal Brief as the fee for filing the original Appeal Brief was paid at submission. However, should any fees be required to file this Compliant Appeal Brief, please charge that fee, as well as any additional required fees, to **IBM Deposit Account No. 09-0457**.

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Michelle Sanderson Date: 04/10/2006 Signature: 

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 011285, frame 0030 et. seq. of the USPTO assignment records.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant, the Appellant's legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 stand finally rejected by the Examiner, as noted in the Final Office Action dated January 19, 2005. The rejection of Claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 is appealed.

STATUS OF AMENDMENTS

Appellant's Amendment A filed on July 7, 2004 was entered by the Examiner as indicated in the Final Office Action. No amendment to the claims was proposed or entered subsequent to the Final Rejection dated January 19, 2005.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellant's invention may be implemented as a method, a system, or a computer program product operable in a dynamic host configuration protocol (DHCP) network that prevents unauthorized dynamic host configuration servers from responding to client configuration requests. The invention uses a designated server checker client that broadcasts configuration requests to draw configuration server responses which are then analyzed to detect unauthorized servers. Detected unauthorized servers are individually targeted by the server checker client with configuration requests to prevent the unauthorized servers from interacting with the network clients.

Appellant's Claim 1 provides a method for "preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an Internet Protocol (IP) network," including the following steps: (1) broadcasting host configuration requests from a server checker client (*see specification* page 18, lines 14-15 and 27-28, describing with reference to FIG. 1 a DHCP client broadcasting a host configuration request, the first part of which is a DHCPDISCOVER message; page 21, lines 14-17, with reference to FIG. 2, describing a server detector component 207 sending requests (via broadcast as described with reference to FIG. 1) to retrieve configuration information); (2) receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests (page 19, lines 1-11, referring to FIG. 1, describing receipt by DHCP client 101 of configuration offer messages in response to the DHCPDISCOVER messages; page 21, lines 14-22, referring to FIG. 2, describing receipt of DHC OFFER messages returned by DHCP servers 203 and 204 responsive to configuration requests sent by checker client 205); (3) detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages (page 21, lines 17-22, referring to FIG. 2, describing invalid server detector 207 detecting one or more unauthorized servers within IP network 202 by comparing a "server identifier" option in the configuration offer messages with authorized server identification data in a DHCP server table 206); and (4) responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients (page 21, line 24 through page 22, line 3, referring to FIG. 2, describing an invalid server denial handler component 208 sending multiple requests (including DHCPDISCOVER messages and the second part of an overall host configuration request called a DHCPREQUEST – *see* page 19, lines 11-17) directed to each detected unauthorized server 204).

The invention recited in Claim 14 provides a system for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an IP network. The system includes: (1) processing means for broadcasting host configuration requests from a server checker client (*see specification* page 18, lines 14-15 and 27-28, describing with reference to FIG. 1 a DHCP client broadcasting a host configuration request, the

first part of which is a DHCPDISCOVER message; page 21, lines 14-17, with reference to FIG. 2, describing a server detector component 207 sending requests (via broadcast as described with reference to FIG. 1) to retrieve configuration information); (2) processing means for receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests (page 19, lines 1-11, referring to FIG. 1, describing receipt by DHCP client 101 of configuration offer messages in response to the DHCPDISCOVER messages; page 21, lines 14-22, referring to FIG. 2, describing receipt of DHC OFFER messages returned by DHCP servers 203 and 204 responsive to configuration requests sent by checker client 205); (3) processing means for detecting an unauthorized dynamic host configuration server within said IP

BEST AVAILABLE COPY